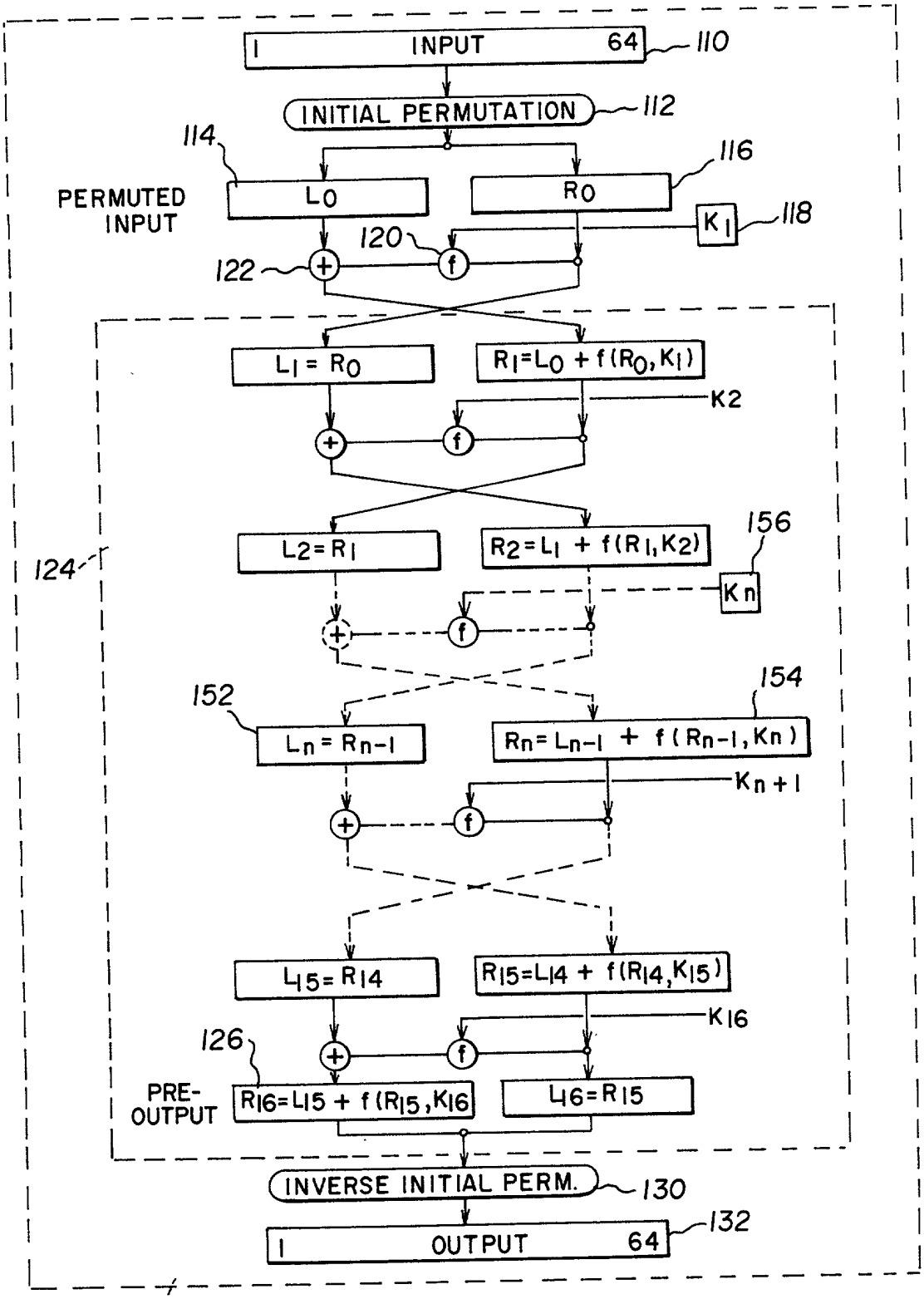

INPUT
64
110
INITIAL PERMUTATION
112
114
116
PERMUTED INPUT
L0
R0
K1
118
120
f
122
L1 = R0
R1=L0 + f(R0,K1)
K2
L2=R1
R2=L1 + f(R1,K2)
156
124
Kn
152
154
Ln = Rn-1
Rn=Ln-1 + f(Rn-1,Kn)
Kn+1
L15=R14
R15=L14 + f(R14,K15)
K16
126
PRE-OUTPUT
R16=L15 + f(R15,K16)
L16=R15
INVERSE INITIAL PERM.
130
OUTPUT
64
132
108

Fig. 1

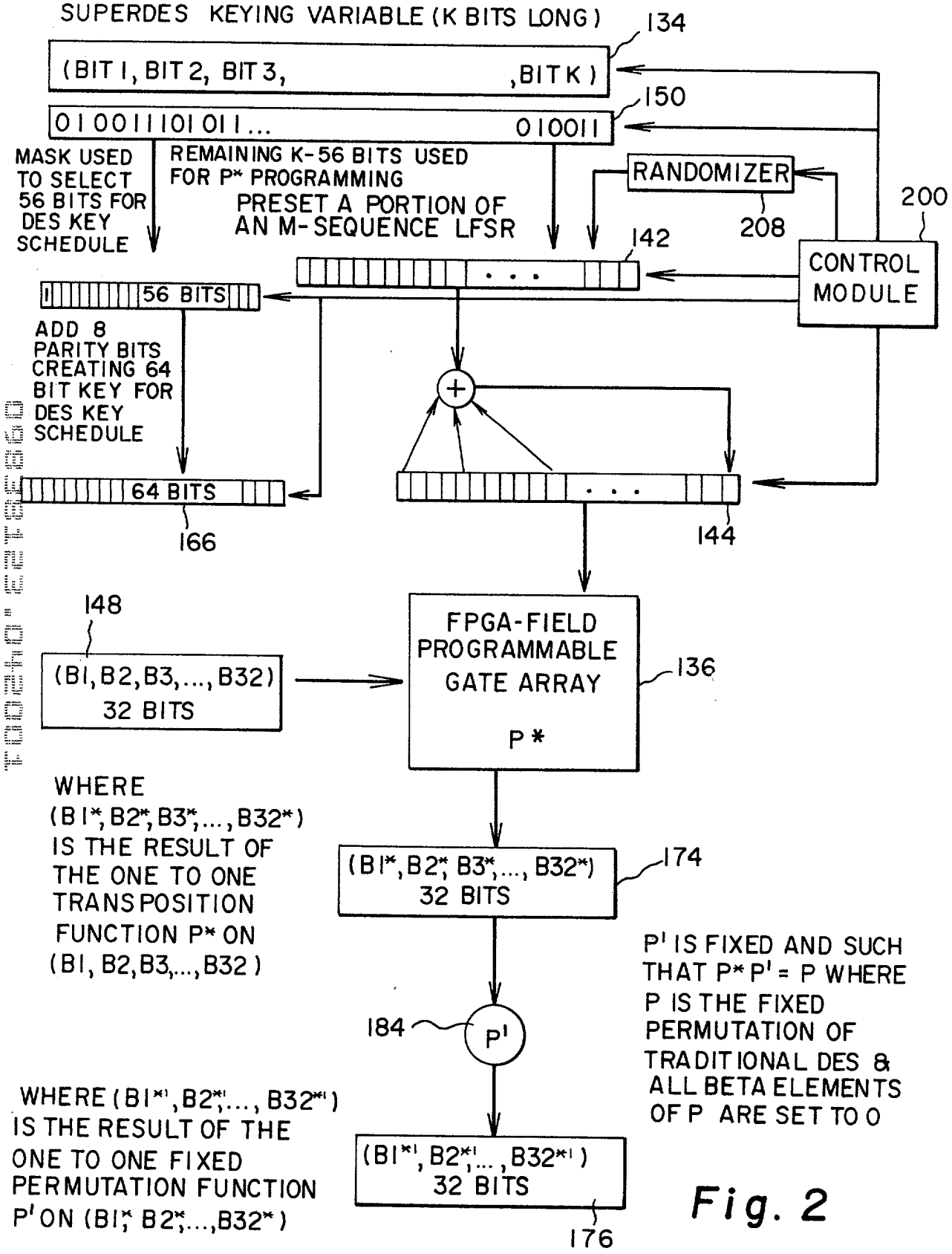

SUPERDES KEYING VARIABLE (K BITS LONG)
134
(BIT 1, BIT 2, BIT 3, ,BIT K)
150
0 1 0 0 1 1 1 0 1 0 1 1 ... 0 1 0 0 1 1
MASK USED TO SELECT 56 BITS FOR DES KEY SCHEDULE
REMAINING K-56 BITS USED FOR P* PROGRAMMING
PRESET A PORTION OF AN M-SEQUENCE LFSR
RANDOMIZER
208
200
142
CONTROL MODULE
56 BITS
ADD 8 PARITY BITS CREATING 64 BIT KEY FOR DES KEY SCHEDULE
64 BITS
166
144
148
(B1, B2, B3, ..., B32)
32 BITS
FPGA-FIELD PROGRAMMABLE GATE ARRAY
P*
136
WHERE (B1*, B2*, B3*, ..., B32*) IS THE RESULT OF THE ONE TO ONE TRANSPOSITION FUNCTION P* ON (B1, B2, B3, ..., B32)
(B1*, B2*, B3*, ..., B32*)
32 BITS
174
P' IS FIXED AND SUCH THAT P* P' = P WHERE P IS THE FIXED PERMUTATION OF TRADITIONAL DES & ALL BETA ELEMENTS OF P ARE SET TO 0
184
P'
WHERE (B1*', B2*', ..., B32*') IS THE RESULT OF THE ONE TO ONE FIXED PERMUTATION FUNCTION P' ON (B1*, B2*, ..., B32*)
(B1*', B2*', ..., B32*')
32 BITS
176

Fig. 2

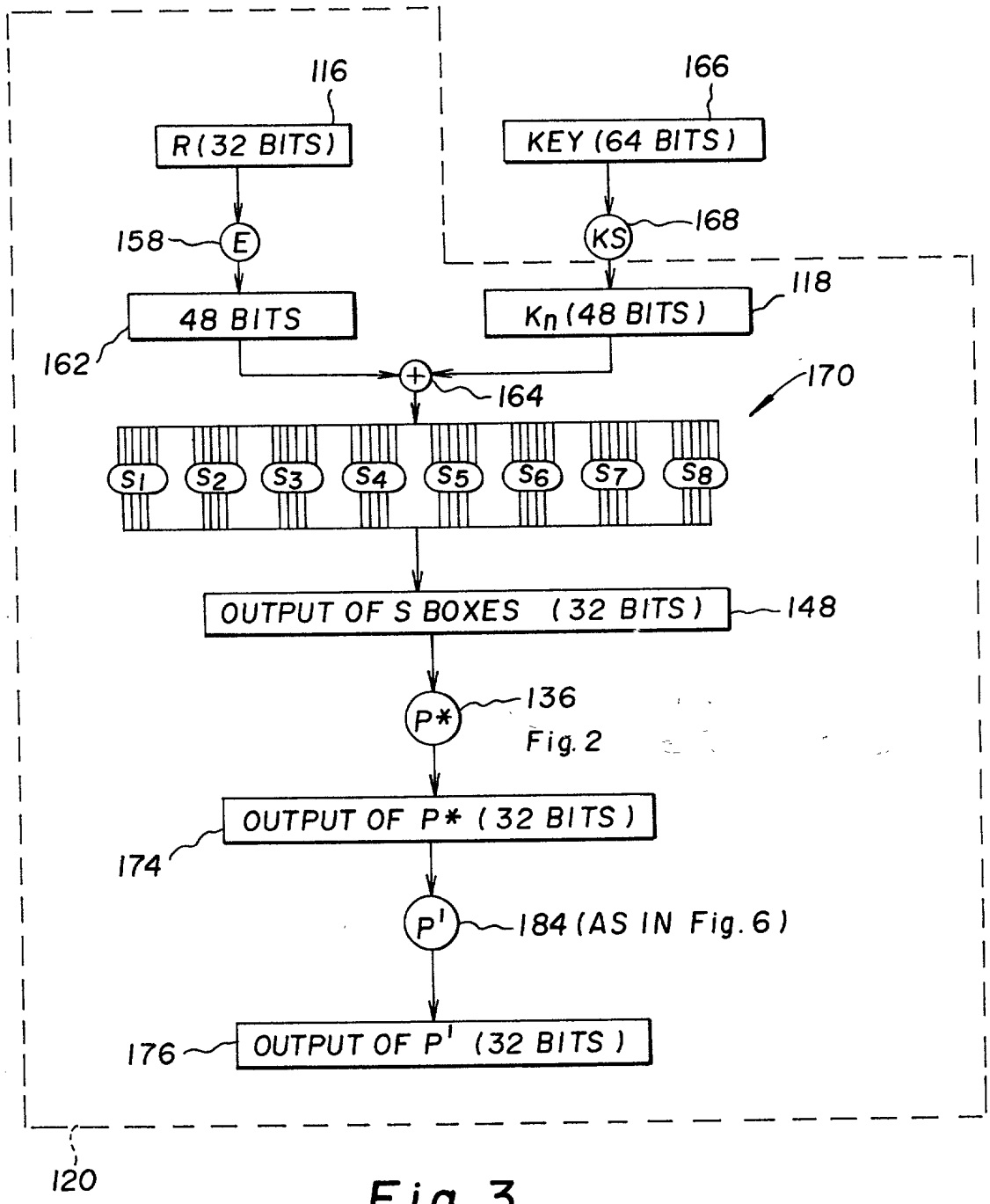

116
R (32 BITS)
166
KEY (64 BITS)
158
E
KS
168
48 BITS
Kn (48 BITS)
118
162
164
170
S1
S2
S3
S4
S5
S6
S7
S8
OUTPUT OF S BOXES (32 BITS)
148
P*
136
Fig. 2
OUTPUT OF P* (32 BITS)
174
P'
184 (AS IN Fig. 6)
176
OUTPUT OF P' (32 BITS)
120

Fig. 3

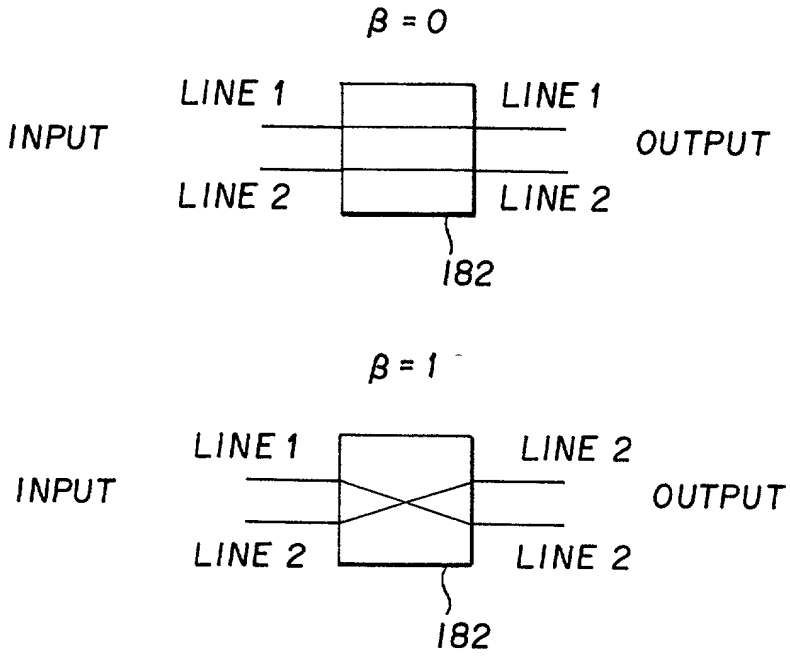

β = 0
LINE 1
LINE 1
INPUT
OUTPUT
LINE 2
LINE 2
182
β = 1
LINE 1
LINE 2
INPUT
OUTPUT
LINE 2
LINE 2
182

Fig. 5

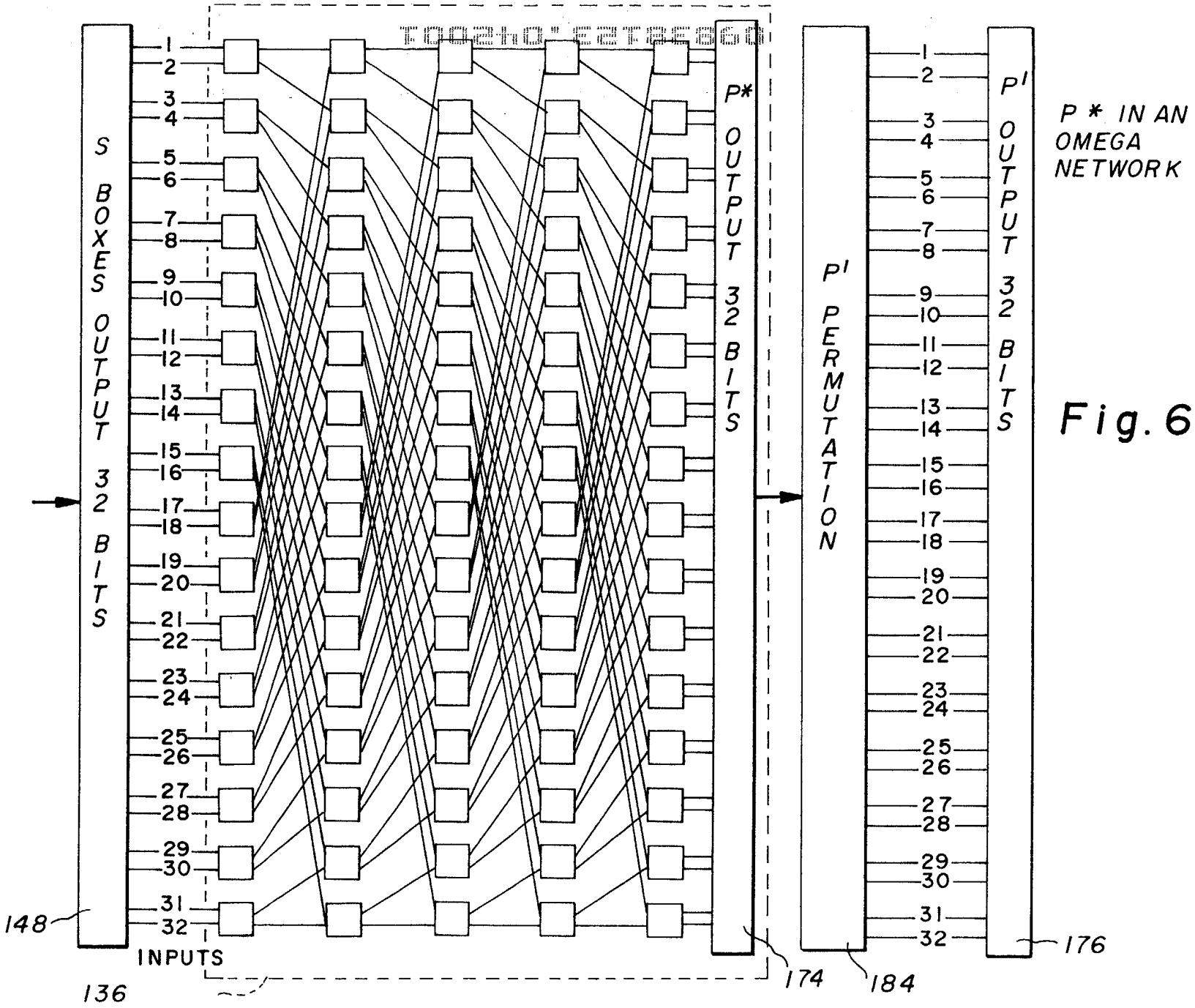

S BOXES OUTPUT 32 BITS
P* OUTPUT 32 BITS
P' PERMUTATION
P' OUTPUT 32 BITS
P * IN AN OMEGA NETWORK
INPUTS
136
148
174
184
176

Fig. 6

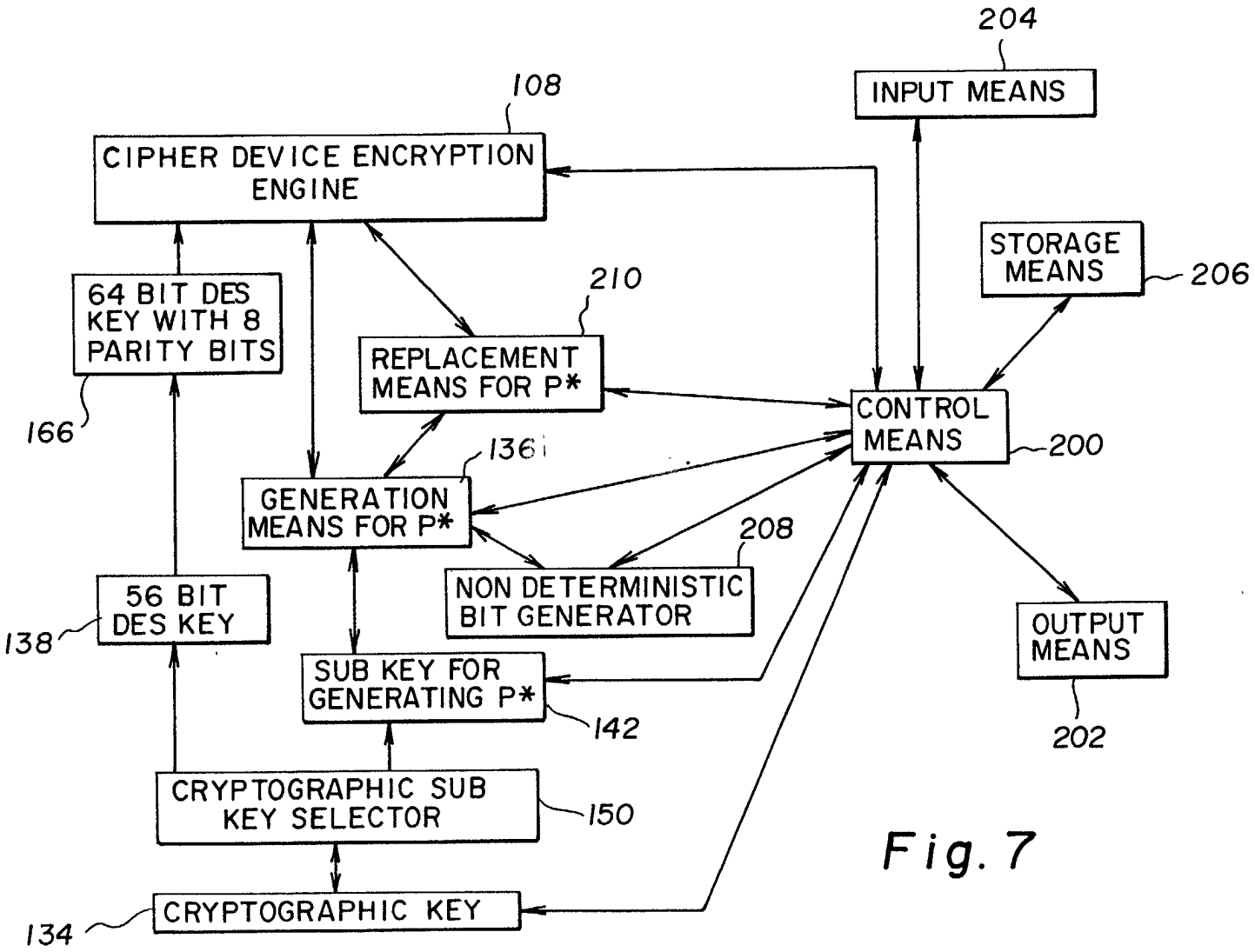
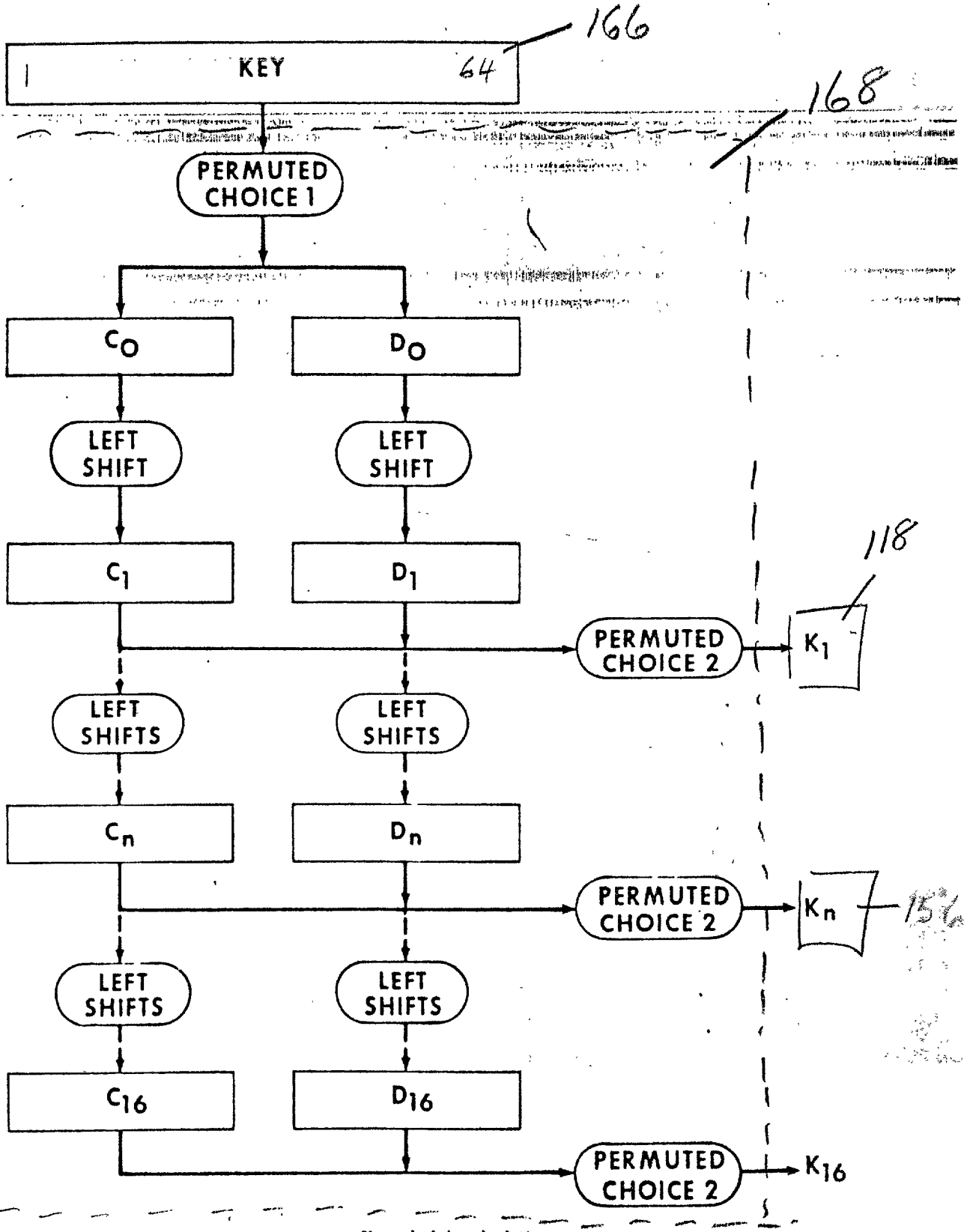


Fig. 7



Key schedule calculation.

Fig 8